Northamptonshire County Council

police

LOCAL SAFEGUARDING CHILDREN BOARD NORTHAMPTONSHIRE

Northamptonshire Local Safeguarding Children Board

Acceptable Use Policy

Revised September 2009- Version 6
Ratified January 2010

CONTENTS

This policy is designed for use by Headteachers, Governors, e-Safety Leaders and the Designated Person for Child Protection, in the first instance.

This Policy should be used in conjunction with Schools Safety Policies.

This policy has been written as a guide for **all schools and educational settings**, where many e-safety risks and management issues are the same, with the same key messages for children, young people, their parents/carers and staff/other users.

It is the responsibility of the establishment to adapt the content of this policy to the needs and curriculum of their children and young people whilst still reflecting the key messages and procedures required to successfully implement this policy.

Using the embc and Enable broadband services as outlined in this policy will ensure your establishment meets the requirements for safeguarding on-line users.

Where comments appear in italics, agencies should decide how to respond and amend the comments accordingly, although any comments are open to amendment. Agencies should amend the policy as is appropriate to their establishment and seek advice, if required.

This policy has been developed by the Childr

What is an AUP (Acceptable Use Policy)?

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within a school or other educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- Webs ites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Learning Platforms
- Video Broadcasting

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. The policy should also provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It explains procedures for any unacceptable use of these technologies by adults, children or young people.

Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies. The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyber-bul lying.
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which is abusive or pornographic

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the school or setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children and young people continue to be protected.

As part of the Every Child Matters agenda set out by the government, the

2 Roles and responsibilities of the school (or establishment):

2.1 Governors and Headteacher *(To be substituted with other relevant staff as required by the establishment.)*

- It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:
- The Headteacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who holds this post within the school.
- *The Headteacher, along with the governors will need to decide if there should be a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school or the LA.*
- Time and resources should be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate. *Establishment to decide how much time to be allocated*.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher should inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors are to be made aware of e-Safety developments from the Curriculum meetings.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-Safety Governor (can be the ICT or Child Protection Governor) ought to challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:
  Challenging the school about having:
  - Firewalls
  - Anti-virus and anti-spyware software
  - Filters
  - Using an accredited ISP (internet Service Provider)
  - Awareness of wireless technology issues
  - A clear policy on using personal devices.

  Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure

2.2 e-Safety Leader

It is the role of the designated e-Safety Leader or Committee (*which could also be the ICT, PSHE or Child Protection Designated Person already in role, but should be a senior member of the school and not a network manager*) to:

- Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform *or ensure the technician is informed and carries out work as directed*.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis. *School to decide how frequently and whether this will be at the Governors Curriculum Meeting.*
- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Transparent monitoring of the internet and on-line technologies - *the school will need to decide here how they wish to monitor the use of the internet and technologies by staff and children and young people.* Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to Section 12 of the Allegation Procedure from the LSCBN to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Work alongside the ICT Leader, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

Ensure that unsolicited e-mails to a member of staff from other sources is minimised o Tone of e-mails is in keeping with all other methods of communication

- (To be reviewed in light of union consultation according to workforce agreements.)

Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

2.3 Staff or adults

- It is the responsibility of all adults within the school or other setting to: Ensure that they know who the Designated Person for Child Protection is within school or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Safeguarding lead. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately. (Following the Allegation Procedure, Section 12, LSCBN.)
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Safeguarding lead immediately, who should then follow the Allegations Procedure, Section 12, LSCBN, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-Safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- *Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices. (This will vary from school to school, but is advisable so that there is staff protection against allegations made by children and young people.)*
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- School bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises. Report accidental access to inappropriate materials to the e-Safety Leader and Synetrix helpdesk in order that inappropriate sites are

added to the restricted list or control this with the Local Control options via your broadband connection.

- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school

3. Appropriate and Inappropriate Use

3.1 By staff of adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff. The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. *Staff training should underpin the receipt of this policy.*

When accessing the Learning Platform from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
Please refer to appendices for a complete list of Acceptable Rules for Staff.
Decide whether these are going to be signed by staff to show acceptance.

In the event of inappropriate use
If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/safeguarding lead immediately and then the Allegations Procedure (Section 12, LSCBN) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted. In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

3.2 By Children or Young People

Acceptable Use Rules and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules should be on display within the classrooms and computer suite, where this may be applicable.

Schools or educational settings should encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

4 The curriculum and tools for Learning

4.1 Internet use

Schools and educational settings should teach children and young people how to use the internet safely and responsibly. They should also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave *Year 6 or Year 11*:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information

Personal safety

An on-line personal space for adapting as a user to:

- upload work
- access calendars and diaries
- blog

The personal space (MySite) is designed to provide young users with the facility to share information and work collaboratively with others members of the Northamptonshire enable community. It should be noted that MySite provides the user with a private area where they may store information about and that a senior member of the team has an overview of potential issues on a regular basis

It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement. Other technologies which schools and settings use with children and young people include:
. photocopiers
. fax machines
. telephones
. PDAs (amend accordingly)

4.6 Video and photographs

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school setting. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.

5. Web 2.0 Technologies

5.1 Managing Social Networking and other Web 2.0 technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and express themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily acccessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, MySpace and Bebo.) In response to this issue the following measures should be put in place:

- The school/educational setting should control access to social networking sites through existing filtering systems. (*Schools utilising the learning platform can access monitored LP+ Quicknote and discussion board tools for collaborative working. Both features sit within the security of the platform and content can be monitored)*
- Students are advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends.)
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos which could reveal personal details (e.g. house number, street name, school uniform)
- Pupils are advised on social networking security and recommendations

incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.

5.2 Social networking advice for staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school email account for homework purposes)
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some schools and other educational settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include EdModo or Virtual Learning Environments such as Moodle which contain similar features.

6. Safeguarding measures

6.1 Filtering

Staff, children and young people are required to use the personalised learning space (enable) and all tools within it, in an acceptable way.
Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate use of the learning platform.

The embc broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All**

The Headteacher should sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from embc-pl. In the event that the site l skin layout for further advice and information

8. School library

The computers in the school library should be protected in line with the school network.
Where software is used that requires a child login, this ought to be password protected so that the child is only able to access themselves as a user. Children and young people should be taught not to share passwords.
The same acceptable use rules apply for any staff and children and young people using this technology.

9. Parents

9.1 Roles

(There is no statutory requirement for parents to sign acceptable use policies but evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful) Each child or young person should receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.
It should be expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

School should keep a record of the signed forms.

9.2 Support

Schools and settings may choose to follow or adapt this guidance:
As part of the approach to developing e-safety awareness with children and young people, the school or setting may offer parents the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school. The school or setting may want to promote a positive attitude to using the World Wide Web and therefore want

10. Links to other policies

10.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. Schools/educational settings should have an up to date Anti-bullying Policy which will include any cyberbullying issues. *All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and young people and their parents/carers.* People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

10.2 Managing allegations and concerns of abuse made against people who work with children.

Please refer to the Allegation Procedure, Section 12 LSCBN, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the designated person for child protection within the school or educational setting immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Managing Allegations team:
For Schools:
Christine Churchman- South Northants cchurchman@northamptonshire.gov.uk 01604654022
Jill Sneddon- North Northants jsneddon@northamptonshire.gov.uk 01536533933
All other settings:
Gerry Barr- gbarr@northamptonshire.gov.uk 01933220708

10.3 PSHE

The teaching and learning of e-Safety should be embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.

10.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

10.5 CCTV

To comply with both the Data Protection Act 1998 and the Information

- should have erected a sign to inform members of the public that they are entering a surveillance area and to display the following key information. The name of the school/individuals responsible for the CCTV system The contact details of who is responsible for the system
-
-

The purpose of the CCTV system

The school must ensure that all images recorded through the CCTV system are fully traceable with the date, time, recording device and person responsible for recording all detailed in a secure log for audit trail purposes. A robust and thoughtful collection of Standard Operating Procedures should be in place to govern the day to day operation of the CCTV system. For data security purposes a restricted number of staff should have access to any images and recordings held by the school. List names here
(*school to decide who would be appropriate e.g. Head teacher or Safeguarding Lead.)*

10.6 School website (if different to the Learning Platform space)
The uploading of images to the school website should be subject to the same acceptable rules as uploading to any personal on-line space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

10.7 External websites
In the event that a member of staff finds themselves or another adult on an

Appendices

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report webs ite to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school: Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately: Ensure the child is reassured and remove them from the situation immediately. Report to the Headteacher and Designated Person for Child Protection immediately. Preserve the information received by the child if possible and
determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

- N.B. There are three incidences when you must report directly to the
- police. Indecent images of children found.
- Incidents of 'grooming' behaviour.

The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the Designated Person for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.

Northamptonshire County Council

police

LOCAL SAFEGUARDING CHILDREN BOARD
NORTHAMPTONSHIRE

e-Safety Acceptable Use Rules Letter to Parents/Carer for Primary or Secondary

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the internet, E-mail and personal on-line space via the East Midlands Broadband Consortium (embc).

In order to support the school in educating your child/young person about e-Safety (safe use of the internet), please read the following Rules with your child/young person then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the e-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the internet and other on-line tools (e.g. mobile phone), both within and beyond

Key Stage 1

These are our rules for using the internet safely.

Our Internet and E-mail Rules

- We use the internet safely to help us learn.
- We learn how to use the internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using our safe internet.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2

These are our rules for using the internet safely and responsibly.

Our On-line Rules

- We use the internet to help us learn and we will learn how to use the internet safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail, chat to or video-conference people an adult has approved.
- Adults are aware when we use on-line tools, such as video-conferencing.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips without permission and never include names with photographs.
- If we need help we know who to ask.
- If we see anything on the internet or in an e-mail that makes us uncomfortable, we know what to do.
-

Key Stage 3 and 4

Secondary e- Safety awareness for students

We are encouraged to use and be aware of the safety rules and procedures which regulate our use of the ICT resources, including INTERNET. At 00000, we are encouraged and allowed to access our curriculum network and the internet, enabling us to use vast resources and communicate, in support of research and education.
We insist that these facilities are used for educational purposes and in an appropriate manner. We are responsible for our behaviour and communication. We know that any breach of the rules will be considered a disciplinary matter.

- **We know access to the networked resources is our privilege. We are encouraged to make use of the internet in support of our studies in all subjects.**
- **We need to make sure we are supervised when we use the internet at school or at home.**
- **We do not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to ourselves and others.**
- **We follow our teacher's instructions carefully.**
- **We must have permission from our parents/carers before we can use the internet for our own independent research at school.**
- **We always work with our friend when we are browsing the Web. We ask "Is it true?" We do not assume that information published on the Web or written in an e-mail is accurate or true.**
- **We keep our username and password private. We do not tell anyone.**
- **When we use e-mail, we only write to 'net pals' or mentors approved by our teacher in school.**
- **We are careful about what we write. We check our work before we print or send anything. We do not use bad language. We do not write racist, sexist, abusive, homophobic or aggressive words. We do not write things that could upset and offend others. We could give ourselves and the school a bad name.**
- **We do not ever give personal information about ourselves and anyone else, such as our address, telephone number and private details in an e-mail or on a Website. We know we could put ourselves or others in danger.**
- **We do not respond to bad e-mail messages. We let our teachers know immediately if we are sent anything we do not feel comfortable with.**
- **We are wise net surfers. We do not go to sites or download any materials, which are offensive, violent and pornographic.**
- **We understand that we are forbidden to use any technology designed to avoid or bypass school filtering controls. We know that these filters are in place to protect us from viewing websites that are unsuitable or unsafe for us.**
- **We always respect the privacy of other users' files.**
- **We will report any incident that breaches the Acceptable Use Policy rules immediately to our teacher.**

> **We know that we can go to www.thinkuknow.co.uk for help.**

Further Information and Guidance

- The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.parentscentre.gov.uk (for parents/carers)

- www.ceop.co.uk (for parents/carers and adults)

- www.iwf.org.uk (for reporting of illegal images or content)

www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults